

National Cyber Alert System

[Archive](#)

Cyber Security Bulletin SB09-355

Vulnerability Summary for the Week of December 14, 2009

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities					
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info	
adobe -- acrobat adobe -- acrobat_reader	Use-after-free vulnerability in the Doc.media.newPlayer method in Adobe Reader and Acrobat 8.0 through 9.2, and possibly earlier versions, allows remote attackers to execute arbitrary code via a crafted PDF file using ZLib compressed streams, as exploited in the wild in December 2009.	2009-12-14	10.0	CVE-2009-4324 XF VUPEN MISC MISC BID MISC SECUNIA OSVDB MISC MISC	
boldfx -- arctic_issue_tracker	SQL injection vulnerability in index.php in Arctic Issue Tracker 2.1.1 allows remote attackers to execute arbitrary SQL commands via the (1) matchings[id] or (2) matchings[title] parameters in a Login action to an unspecified program, or (3) the matchings[id] parameter in a search action to index.php, a different	2009-12-17	7.5	CVE-2009-4350 SECUNIA MISC OSVDB	

	vector than CVE-2008-3250. NOTE: some of these details are obtained from third party information.			
ibm -- db2	Unspecified vulnerability in db2licm in the Engine Utilities component in IBM DB2 9.5 before FP5 has unknown impact and local attack vectors.	2009-12-16	7.2	CVE-2009-4330 CONFIRM
ibm -- db2	The Install component in IBM DB2 9.5 before FP5 and 9.7 before FP1 configures the High Availability (HA) scripts with incorrect file-permission and authorization settings, which has unknown impact and local attack vectors.	2009-12-16	7.2	CVE-2009-4331 CONFIRM AIXAPAR
ibm -- db2	The Relational Data Services component in IBM DB2 9.5 before FP5 allows attackers to obtain the password argument from the SET ENCRYPTION PASSWORD statement via vectors involving the GET SNAPSHOT FOR DYNAMIC SQL command.	2009-12-16	7.5	CVE-2009-4333 CONFIRM
ibm -- db2	Multiple unspecified vulnerabilities in bundled stored procedures in the Spatial Extender component in IBM DB2 9.5 before FP5 have unknown impact and remote attack vectors, related to "remote exploits."	2009-12-16	10.0	CVE-2009-4335 VUPEN CONFIRM
jean-david_gadina -- slideshow	SQL injection vulnerability in the Flash SlideShow (slideshow) extension 0.2.2 for TYPO3 allows remote attackers to execute arbitrary SQL commands via unknown vectors.	2009-12-17	7.5	CVE-2009-4338 XF VUPEN CONFIRM
linux -- kernel	The EXT4_IOC_MOVE_EXT (aka move extents) ioctl implementation in the ext4 filesystem in the Linux kernel before 2.6.32-git6 allows local users to overwrite arbitrary files via a crafted request, related to insufficient checks for file permissions.	2009-12-12	7.2	CVE-2009-4131 CONFIRM VUPEN BID CONFIRM MLIST

melvin_mach -- jobexchange	SQL injection vulnerability in the Job Exchange (jobexchange) extension 0.0.3 for TYPO3 allows remote attackers to execute arbitrary SQL commands via unknown vectors.	2009-12-17	7.5	CVE-2009-4342 XF VUPEN CONFIRM
microsoft -- windows_2000 microsoft -- windows_2003_server microsoft -- windows_xp	Unspecified vulnerability in the Indeo codec in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 allows remote attackers to execute arbitrary code via crafted media content, as reported to Microsoft by Paul Byrne of NGS Software. NOTE: this might overlap CVE-2008-3615.	2009-12-12	9.3	CVE-2009-4311 CONFIRM MSKB MSKB MSKB
mischa_heissmann -- no_indexed_search	SQL injection vulnerability in the No indexed Search (no_indexed_search) extension 0.2.0 for TYPO3 allows remote attackers to execute arbitrary SQL commands via unknown vectors.	2009-12-17	7.5	CVE-2009-4341 XF VUPEN CONFIRM
moodle -- moodle	Moodle 1.8 before 1.8.11 and 1.9 before 1.9.7 does not use a random password salt in config.php, which makes it easier for attackers to conduct brute-force password guessing attacks.	2009-12-15	7.5	CVE-2009-4304 VUPEN BID CONFIRM CONFIRM CONFIRM
mozilla -- firefox mozilla -- seamonkey	liboggplay in Mozilla Firefox 3.5.x before 3.5.6 and SeaMonkey before 2.0.1 might allow context-dependent attackers to cause a denial of service (application crash) or execute arbitrary code via unspecified vectors, related to "memory safety issues."	2009-12-17	9.3	CVE-2009-3388 VUPEN
mozilla -- firefox mozilla -- seamonkey	Integer overflow in libtheora in Xiph.Org Theora before 1.1, as used in Mozilla Firefox 3.5 before 3.5.6 and SeaMonkey before 2.0.1, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a video with large dimensions.	2009-12-17	9.3	CVE-2009-3389 VUPEN CONFIRM

mozilla -- firefox mozilla -- seamonkey	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 3.0.16 and 3.5.x before 3.5.6, SeaMonkey before 2.0.1, and Thunderbird allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	2009-12-17	9.3	CVE-2009-3979 CONFIRM
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 3.5.x before 3.5.6, SeaMonkey before 2.0.1, and Thunderbird allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	2009-12-17	9.3	CVE-2009-3980 VUPEN CONFIRM
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	Unspecified vulnerability in the browser engine in Mozilla Firefox before 3.0.16, SeaMonkey before 2.0.1, and Thunderbird allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	2009-12-17	9.3	CVE-2009-3981 CONFIRM
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	Multiple unspecified vulnerabilities in the JavaScript engine in Mozilla Firefox 3.5.x before 3.5.6, SeaMonkey before 2.0.1, and Thunderbird allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	2009-12-17	9.3	CVE-2009-3982 VUPEN VUPEN CONFIRM
mozilla -- firefox mozilla -- seamonkey	Mozilla Firefox before 3.0.16 and 3.5.x before 3.5.6, and SeaMonkey before 2.0.1, allows remote attackers to execute arbitrary JavaScript with chrome privileges by leveraging a reference to a chrome window from a content	2009-12-17	7.6	CVE-2009-3986 VUPEN SECTRACK SECTRACK

	window, related to the window.opener property.			
mozilla -- firefox mozilla -- seamonkey	The GeckoActiveXObject function in Mozilla Firefox before 3.0.16 and 3.5.x before 3.5.6, and SeaMonkey before 2.0.1, generates different exception messages depending on whether the referenced COM object is listed in the registry, which allows remote attackers to obtain potentially sensitive information about installed software by making multiple calls that specify the ProgID values of different COM objects.	2009-12-17	7.8	CVE-2009-3987 VUPEN SECTRACK SECTRACK
ruby-lang -- ruby	Heap-based buffer overflow in the rb_str_justify function in string.c in Ruby 1.9.1 before 1.9.1-p376 allows context-dependent attackers to execute arbitrary code via unspecified vectors involving (1) String#ljust, (2) String#center, or (3) String#rjust. NOTE: some of these details are obtained from third party information.	2009-12-11	10.0	CVE-2009-4124 CONFIRM
simon_rundell -- pd_calendar_today	SQL injection vulnerability in the Diocese of Portsmouth Calendar (pd_calendar) extension 0.4.1 and earlier for TYPO3 allows remote attackers to execute arbitrary SQL commands via unknown vectors, a different issue than CVE-2008-6691.	2009-12-17	7.5	CVE-2009-4337 XF VUPEN CONFIRM
stephan_vits -- mf_subscription	SQL injection vulnerability in the Subscription (mf_subscription) extension 0.2.2 for TYPO3 allows remote attackers to execute arbitrary SQL commands via unknown vectors.	2009-12-17	7.5	CVE-2009-4339 XF VUPEN CONFIRM
	VRTSweb.exe in VRTSweb in Symantec Backup Exec Continuous Protection Server (CPS) 11d, 12.0, and 12.5; Veritas NetBackup Operations Manager (NOM) 6.0 GA through			

symantec -- backup_exec_continuous_protection_server symantec -- veritas_application_director symantec -- veritas_backup_exec symantec -- veritas_cluster_server symantec -- veritas_cluster_server_management_console symantec -- veritas_cluster_server_one symantec -- veritas_command_central_enterprise_reporter symantec -- veritas_command_central_storage symantec -- veritas_command_central_storage_change_manager symantec -- veritas_micromeasure symantec -- veritas_netbackup_operations_manager symantec -- veritas_netbackup_reporter symantec -- veritas_storae_foundation symantec -- veritas_storage_foundation symantec -- veritas_storage_foundation_cluster_file_system symantec -- veritas_storage_foundation_cluster_file_system_for_oracle_rac symantec -- veritas_storage_foundation_for_db2 symantec -- veritas_storage_foundation_for_high_availability symantec -- veritas_storage_foundation_for_oracle symantec -- veritas_storage_foundation_for_oracle_real_application_cluster symantec -- veritas_storage_foundation_for_sybase symantec -- veritas_storage_foundation_for_windows_high_availability symantec -- veritas_storage_foundation_manager	6.5.5; Veritas Backup Reporter (VBR) 6.0 GA through 6.6; Veritas Storage Foundation (SF) 3.5; Veritas Storage Foundation for Windows High Availability (SFWHA) 4.3MP2, 5.0, 5.0RP1a, 5.0RP2, 5.1, and 5.1AP1; Veritas Storage Foundation for High Availability (SFHA) 3.5; Veritas Storage Foundation for Oracle (SFO) 4.1, 5.0, and 5.0.1; Veritas Storage Foundation for DB2 4.1 and 5.0; Veritas Storage Foundation for Sybase 4.1 and 5.0; Veritas Storage Foundation for Oracle Real Application Cluster (SFRAC) 3.5, 4.0, 4.1, and 5.0; Veritas Storage Foundation Manager (SFM) 1.0, 1.0 MP1, 1.1, 1.1.1UX, 1.1.1Win, and 2.0; Veritas Cluster Server (VCS) 3.5, 4.0, 4.1, and 5.0; Veritas Cluster Server One (VCSOne) 2.0, 2.0.1, and 2.0.2; Veritas Application Director (VAD) 1.1 and 1.1 Platform Expansion; Veritas Cluster Server Management Console (VCSMC) 5.1, 5.5, and 5.5.1; Veritas Storage Foundation Cluster File System (SFCFS) 3.5, 4.0, 4.1, and 5.0; Veritas Storage Foundation Cluster File System for Oracle RAC (SFCFS RAC) 5.0; Veritas Command Central Storage (CCS) 4.x, 5.0, and 5.1; Veritas Command Central Enterprise Reporter (CC-ER) 5.0 GA, 5.0 MP1, 5.0 MP1RP1, and 5.1; Veritas Command Central Storage Change Manager (CC-SCM) 5.0 and 5.1; and Veritas MicroMeasure 5.0 does not properly validate authentication requests, which allows remote attackers to trigger the unpacking of a WAR archive, and execute arbitrary code in the contained files, via	2009-12-11	10.0	CVE-2009-3027 MISC CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM HP HP

	crafted data to TCP port 14300.			
transware -- active_mail_2003	The Mobile Edition of TransWARE Active! mail 2003 build 2003.0139.0871 and earlier, and possibly other versions before 2003.0139.0911, does not remove the session ID in a Referer URL, which allows remote attackers to hijack web sessions via vectors such as an email with an embedded URL.	2009-12-17	7.5	CVE-2009-4353 XF CONFIRM SECUNIA JVNDB JVN
windows -- media_player microsoft -- windows_2000 microsoft -- windows_2003_server microsoft -- windows_xp	Stack-based buffer overflow in the Intel Indeo41 codec for Windows Media Player in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 allows remote attackers to execute arbitrary code via crafted compressed video data in an IV41 stream in a media file, leading to many loop iterations, as demonstrated by data in an AVI file.	2009-12-12	9.3	CVE-2009-4310 CONFIRM MSKB MSKB MSKB SECTRACK
zen-cart -- zen_cart	The installation for Zen Cart stores sensitive information and insecure programs under the (1) docs, (2) extras, and (3) xc_install folders, and (4) install.txt, which allows remote attackers to obtain sensitive information, delete the database, and conduct other attacks via a direct request, different vulnerabilities than CVE-2009-4321 and CVE-2009-4322.	2009-12-14	7.5	CVE-2009-4323 CONFIRM

[Back to top](#)

Medium Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source Patch
dominic_eckart -- trainincdb	Cross-site scripting (XSS) vulnerability in the Training Company Database (trainincdb) extension 0.4.7 for TYPO3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-12-17	4.3	CVE-2009-4343 XF VUPEN CONFIRM
eocms -- eocms	PHP remote file inclusion vulnerability in js/bbcodepress/bbcode-form.php in eoCMS 0.9.03 and earlier, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the BBCODE_path parameter.	2009-12-14	6.8	CVE-2009-4319 MISC SECURITY

gnu -- coreutils	The distcheck rule in dist-check.mk in GNU coreutils 5.2.1 through 8.1 allows local users to gain privileges via a symlink attack on a file in a directory tree under /tmp.	2009-12-11	4.4	CVE-2 4135 CONF] MLIST MLIST SECUR MLIST
haroldbakker -- hb-ns	Cross-site scripting (XSS) vulnerability in index.php in Harold Bakker's NewsScript (HB-NS) 1.3 allows remote attackers to inject arbitrary web script or HTML via the topic parameter in a topic action, a different vector than CVE-2006-2146.	2009-12-17	4.3	CVE-2 4348 MISC SECUR
ibm -- db2	The Client Interfaces component in IBM DB2 8.2 before FP18, 9.1 before FP8, 9.5 before FP5, and 9.7 before FP1 does not validate an unspecified pointer, which allows attackers to overwrite "external memory" via unknown vectors, related to a missing "check for null pointers."	2009-12-16	6.4	CVE-2 4325 CONF] CONF]
ibm -- db2	The RAND scalar function in the Common Code Infrastructure component in IBM DB2 9.5 before FP5 and 9.7 before FP1, when the Database Partitioning Feature (DPF) is used, produces "repeating" return values, which might allow attackers to defeat protection mechanisms based on randomization by predicting a value.	2009-12-16	4.3	CVE-2 4326 CONF]
ibm -- db2	The Common Code Infrastructure component in IBM DB2 9.5 before FP5 and 9.7 before FP1 does not properly validate the size of a memory pool during a creation attempt, which allows attackers to cause a denial of service (memory consumption) via unspecified vectors.	2009-12-16	5.0	CVE-2 4327 CONF]
ibm -- db2	Unspecified vulnerability in the DRDA Services component in IBM DB2 9.5 before FP5 allows remote authenticated users to cause a denial of service (server trap) by calling a SQL stored procedure in unknown circumstances.	2009-12-16	4.0	CVE-2 4328 CONF]
ibm -- db2	Unspecified vulnerability in the Engine Utilities component in IBM DB2 9.5 before FP5 allows remote authenticated users to cause a denial of service (segmentation fault) by modifying the db2ra data stream sent in a request from the Load Utility.	2009-12-16	4.0	CVE-2 4329 CONF]
ibm -- db2	db2pd in the Problem Determination component in IBM DB2 9.1 before FP7 and 9.5 before FP5 allows attackers to cause a denial of service (NULL pointer dereference and application termination) via unspecified vectors.	2009-12-16	5.0	CVE-2 4332 CONF] CONF]
ibm -- db2	The Self Tuning Memory Manager (STMM) component in IBM DB2 9.1 before FP8, 9.5 before FP5, and 9.7 before FP1 uses 0666 permissions for the STMM log file, which allows local users to cause a denial of service or have unspecified other impact by writing to this file.	2009-12-16	4.6	CVE-2 4334 CONF]
jonas_renggli -- vshoutbox	Cross-site scripting (XSS) vulnerability in the vShoutbox (vshoutbox) extension 0.0.1 for TYPO3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-12-17	4.3	CVE-2 4345 XF VUPEI CONF]
	drivers/firewire/ohci.c in the Linux kernel before 2.6.32-git9, when packet-per-buffer mode is used, allows local users to cause a denial of			CVE-2 4138

linux -- kernel	service (NULL pointer dereference and system crash) or possibly have unknown other impact via an unspecified ioctl associated with receiving an ISO packet that contains zero in the payload-length field.	2009-12-16	4.7	CONF MLIST CONF CONF
liran_tal -- daloradius	Cross-site scripting (XSS) vulnerability in daloradius-users/login.php in daloRADIS 0.9-8 and earlier allows remote attackers to inject arbitrary web script or HTML via the error parameter.	2009-12-17	4.3	CVE-2 4347 BUGT SECUT MISC
lythgoes -- the_next_generation_of_genealogy_sitebuilding	Cross-site scripting (XSS) vulnerability in searchform.php in The Next Generation of Genealogy Sitebuilding (TNG) 7.1.2 allows remote attackers to inject arbitrary web script or HTML via the msg parameter.	2009-12-14	4.3	CVE-2 4320 XF MISC SECUT
mischa_heissmann -- no_indexed_search	Cross-site scripting (XSS) vulnerability in the No indexed Search (no_indexed_search) extension 0.2.0 for TYPO3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-12-17	4.3	CVE-2 4340 XF VUPEI CONF
moodle -- moodle	Multiple cross-site request forgery (CSRF) vulnerabilities in Moodle 1.8 before 1.8.11 and 1.9 before 1.9.7 allow remote attackers to hijack the authentication of unspecified victims via unknown vectors.	2009-12-15	6.8	CVE-2 4297 VUPEI BID CONF CONF CONF
moodle -- moodle	The LAMS module (mod/lams) for Moodle 1.8 before 1.8.11 and 1.9 before 1.9.7 stores the (1) username, (2) firstname, and (3) lastname fields within the user table, which allows attackers to obtain user account information via unknown vectors.	2009-12-15	5.0	CVE-2 4298 VUPEI BID CONF CONF CONF
moodle -- moodle	mod/glossary/showentry.php in the Glossary module for Moodle 1.8 before 1.8.11 and 1.9 before 1.9.7 does not properly perform access control, which allows attackers to read unauthorized Glossary entries via unknown vectors.	2009-12-15	5.0	CVE-2 4299 VUPEI BID CONF CONF CONF
moodle -- moodle	Multiple unspecified authentication plugins in Moodle 1.8 before 1.8.11 and 1.9 before 1.9.7 store the MD5 hashes for passwords in the user table, even when the cached hashes are not used by the plugin, which might make it easier for attackers to obtain credentials via unspecified vectors.	2009-12-15	5.0	CVE-2 4300 VUPEI BID CONF CONF CONF
moodle -- moodle	mnet/lib.php in Moodle 1.8 before 1.8.11 and 1.9 before 1.9.7, when MNET services are enabled, does not properly check permissions, which allows remote authenticated servers to execute arbitrary MNET functions.	2009-12-15	6.0	CVE-2 4301 BID CONF CONF CONF CONF CONF
moodle -- moodle	login/index_form.html in Moodle 1.8 before 1.8.11 and 1.9 before 1.9.7 links to an index page on the HTTP port even when the page is served from an HTTPS port, which might cause login credentials to be sent in cleartext, even when SSL is intended and allows remote attackers to	2009-12-15	5.0	CVE-2 4302 FEDO FEDO FEDO VUPEI BID

	is intended, and allows remote attackers to obtain these credentials by sniffing.			CONF CONF CONF]
moodle -- moodle	Moodle 1.8 before 1.8.11 and 1.9 before 1.9.7 stores (1) password hashes and (2) unspecified "secrets" in backup files, which might allow attackers to obtain sensitive information.	2009-12-15	5.0	CVE-2 4303 VUPEI BID CONF] CONF] CONF]
moodle -- moodle	SQL injection vulnerability in the SCORM module in Moodle 1.8 before 1.8.11 and 1.9 before 1.9.7 allows remote authenticated users to execute arbitrary SQL commands via vectors related to an "escaping issue when processing AICC CRS file (Course_Title)."	2009-12-15	6.5	CVE-2 4305 VUPEI BID CONF] CONF] CONF]
mozilla -- firefox	Race condition in Mozilla Firefox allows remote attackers to produce a JavaScript message with a spoofed domain association by writing the message in between the document request and document load for a web page in a different domain.	2009-12-14	5.8	CVE-2 4129 XF BID SECTF BUGT]
mozilla -- firefox	Visual truncation vulnerability in the MakeScriptDialogTitle function in nsGlobalWindow.cpp in Mozilla Firefox allows remote attackers to spoof the origin domain name of a script via a long name.	2009-12-14	5.8	CVE-2 4130 XF BID SECTF BUGT]
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	Mozilla Firefox before 3.0.16 and 3.5.x before 3.5.6, and SeaMonkey before 2.0.1, allows remote attackers to send authenticated requests to arbitrary applications by replaying the NTLM credentials of a browser user.	2009-12-17	6.8	CVE-2 3983 VUPEI CONF]
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	Mozilla Firefox before 3.0.16 and 3.5.x before 3.5.6, and SeaMonkey before 2.0.1, allows remote attackers to spoof an SSL indicator for an http URL or a file URL by setting document.location to an https URL corresponding to a site that responds with a No Content (aka 204) status code and an empty body.	2009-12-17	6.8	CVE-2 3984 VUPEI CONF]
mozilla -- firefox mozilla -- seamonkey	Mozilla Firefox before 3.0.16 and 3.5.x before 3.5.6, and SeaMonkey before 2.0.1, allows remote attackers to associate spoofed content with an invalid URL by setting document.location to this URL, and then writing arbitrary web script or HTML to the associated blank document, a related issue to CVE-2009-2654.	2009-12-17	6.8	CVE-2 3985 XF VUPEI SECTF
nuggetz -- nuggetz_cms	Directory traversal vulnerability in admin/ajaxsave.php in Nuggetz CMS 1.0, when magic_quotes_gpc is disabled, allows remote attackers to create or modify arbitrary files via a .. (dot dot) in the nugget parameter and a modified pagevalue parameter, as demonstrated by creating and accessing a .php file to execute arbitrary PHP code.	2009-12-14	6.8	CVE-2 4315 XF CONF] SECUR MISC OSVDI
phpwebscripts -- link_up_gold	Cross-site request forgery (CSRF) vulnerability in administration/administrators.php in Link Up Gold 5.0 allows remote attackers to hijack the authentication of administrators for requests that create administrative accounts.	2009-12-17	6.8	CVE-2 4349 XF VUPEI MISC SECUR MISC

				OSVDI
postgresql -- postgresql	PostgreSQL 7.4.x before 7.4.27, 8.0.x before 8.0.23, 8.1.x before 8.1.19, 8.2.x before 8.2.15, 8.3.x before 8.3.9, and 8.4.x before 8.4.2 does not properly handle a '\o' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which (1) allows man-in-the-middle attackers to spoof arbitrary SSL-based PostgreSQL servers via a crafted server certificate issued by a legitimate Certification Authority, and (2) allows remote attackers to bypass intended client-hostname restrictions via a crafted client certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.	2009-12-15	5.8	CVE-2 4034 CONF] CONF] CONF] CONF] CONF] CONF] CONF]
postgresql -- postgresql	PostgreSQL 7.4.x before 7.4.27, 8.0.x before 8.0.23, 8.1.x before 8.1.19, 8.2.x before 8.2.15, 8.3.x before 8.3.9, and 8.4.x before 8.4.2 does not properly manage session-local state during execution of an index function by a database superuser, which allows remote authenticated users to gain privileges via a table with crafted index functions, as demonstrated by functions that modify (1) search_path or (2) a prepared statement, a related issue to CVE-2007-6600 and CVE-2009-3230.	2009-12-15	6.5	CVE-2 4136 CONF] CONF] CONF] CONF] CONF] CONF] CONF]
realestatephp -- real_estate_manager	Cross-site scripting (XSS) vulnerability in index.php in Real Estate Manager 1.0.1 allows remote attackers to inject arbitrary web script or HTML via the lang parameter. NOTE: some of these details are obtained from third party information.	2009-12-14	4.3	CVE-2 4318 VUPEI MISC SECUT MISC
redhat -- jboss_enterprise_application_platform	Cross-site scripting (XSS) vulnerability in JMX-Console in JBossAs in Red Hat JBoss Enterprise Application Platform (aka JBoss EAP or JBEAP) 4.2 before 4.2.0.CP08 and 4.3 before 4.3.0.CP07 allows remote attackers to inject arbitrary web script or HTML via the filter parameter, related to the key property and the position of quote and colon characters.	2009-12-15	4.3	CVE-2 1380 CONF]
redhat -- jboss_enterprise_application_platform	Multiple cross-site scripting (XSS) vulnerabilities in the Web Console in the Application Server in Red Hat JBoss Enterprise Application Platform (aka JBoss EAP or JBEAP) 4.2.0 before 4.2.0.CP08, 4.2.2GA, 4.3 before 4.3.0.CP07, and 5.1.0GA allow remote attackers to inject arbitrary web script or HTML via the (1) monitorName, (2) objectName, (3) attribute, or (4) period parameter to createSnapshot.jsp, or the (5) monitorName, (6) objectName, (7) attribute, (8) threshold, (9) period, or (10) enabled parameter to createThresholdMonitor.jsp. NOTE: some of these details are obtained from third party information.	2009-12-15	4.3	CVE-2 2405 REDH REDH REDH REDH CONF]
ruby_on_rails -- ruby_on_rails	Ruby on Rails 2.1 before 2.1.3 and 2.2.x before 2.2.2 does not verify tokens for requests with certain content types, which allows remote attackers to bypass cross-site request forgery (CSRF) protection for requests to applications that rely on this protection, as demonstrated using text/plain.	2009-12-15	6.8	CVE-2 7248 VUPEI MISC MLIST MLIST CONF] SECUT MISC MISC

scriptsez -- ez_cart	Cross-site scripting (XSS) vulnerability in index.php in ScriptsEz Ez Cart allows remote attackers to inject arbitrary web script or HTML via the sid parameter in a showcata action.	2009-12-14	4.3	CVE-2 4317 VUPEI MISC SECUR MISC
simon_rundell -- pd_calendar_today	Cross-site scripting (XSS) vulnerability in the Diocese of Portsmouth Calendar (pd_calendar) extension 0.4.1 and earlier for TYPO3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-12-17	4.3	CVE-2 4336 XF VUPEI CONF]
sun -- ray_server_software	Sun Ray Server Software 4.1 on Solaris 10, when Automatic Multi-Group Hotdesking (AMGH) is enabled, responds to a logout action by immediately logging the user in again, which makes it easier for physically proximate attackers to obtain access to a session by going to an unattended DTU device.	2009-12-14	4.4	CVE-2 4314 SUNAI CONF]
tobias_sommer -- zid_linklist	Cross-site scripting (XSS) vulnerability in the ZID Linkliste (zid_linklist) extension 1.0.0 for TYPO3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-12-17	4.3	CVE-2 4344 XF VUPEI CONF]
toni_milovan -- fe_rtenews	Cross-site scripting (XSS) vulnerability in the Frontend news submitter with RTE (fe_rtenews) extension 1.4.1 and earlier for TYPO3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-12-17	4.3	CVE-2 4346 VUPEI CONF]
transware -- active_mail_2003	Multiple cross-site scripting (XSS) vulnerabilities in TransWARE Active! mail 2003 build 2003.0139.0871 and earlier, and possibly other versions before 2003.0139.0939, allow remote attackers to inject arbitrary web script or HTML via the (1) From, (2) To, (3) Cc, and (4) Bcc parameters.	2009-12-17	4.3	CVE-2 4352 XF CONF SECUR JVNDI JVN
transware -- active_mail_2003	TransWARE Active! mail 2003 build 2003.0139.0871 and earlier does not properly secure the session ID in a session cookie, which allows remote attackers to hijack web sessions, probably related to the "secure" flag for cookies in SSL sessions.	2009-12-17	4.3	CVE-2 4354 XF CONF] JVNDI JVN
vmware -- esx_server vmware -- lab_manager vmware -- server vmware -- stage_manager vmware -- vcenter vmware -- vcenter_lab_manager vmware -- vcenter_stage_manager webworks -- epublisher webworks -- help webworks -- publisher	Multiple cross-site scripting (XSS) vulnerabilities in WebWorks Help 2.0 through 5.0 in VMware vCenter 4.0 before Update 1 Build 208156; VMware Server 2.0.2; VMware ESX 4.0; VMware Lab Manager 2.x; VMware vCenter Lab Manager 3.x and 4.x before 4.0.1; VMware Stage Manager 1.x before 4.0.1; WebWorks Publisher 6.x through 8.x; WebWorks Publisher 2003; and WebWorks ePublisher 9.0.x through 9.3, 2008.1 through 2008.4, and 2009.x before 2009.3 allow remote attackers to inject arbitrary web script or HTML via (1) wwhelp_entry.html, reachable through index.html and wwhsec.htm, (2) wwhelp/wwimpl/api.htm, (3) wwhelp/wwimpl/common/html/frameset.htm, (4) wwhelp/wwimpl/common/scripts/switch.js, or (5) the window.opener component in wwhelp/wwimpl/common/html/bookmark.htm, related to (a) unspecified parameters and (b) messages used in topic links for the bookmarking functionality.	2009-12-16	4.3	CVE-2 3731 CONF] BID
				CVE-2 4351

wscreator -- wscreator	SQL injection vulnerability in ADMIN/loginaction.php in WSCreator 1.1, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the Email (aka username) parameter.	2009-12-17	6.8	4351 XF VUPEI BUGT] MISC SECUR OSVDI
zeeways -- zeelyrics	Cross-site scripting (XSS) vulnerability in searchresults_main.php in ZeeLyrics 3x allows remote attackers to inject arbitrary web script or HTML via the keyword parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-12-14	4.3	CVE-2 4316 SECUR
zen-cart -- zen_cart	extras/curltest.php in Zen Cart 1.3.8 and 1.3.8a, and possibly other versions, allows remote attackers to read arbitrary files via a file:// URL. NOTE: some of these details are obtained from third party information.	2009-12-14	5.0	CVE-2 4321 XF MISC VUPEI BID BUGT] MISC SECUR OSVDI
zen-cart -- zen_cart	extras/ipn_test_return.php in Zen Cart allows remote attackers to obtain sensitive information via a direct request, which reveals the installation path in an error message.	2009-12-14	5.0	CVE-2 4322 MISC BUGT] MISC

[Back to top](#)

Low Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
redhat -- jboss_enterprise_application_platform	Twiddle in Red Hat JBoss Enterprise Application Platform (aka JBoss EAP or JBEAP) 4.2 before 4.2.0.CP08 and 4.3 before 4.3.0.CP07 writes the JMX password, and other command-line arguments, to the twiddle.log file, which allows local users to obtain sensitive information by reading this file.	2009-12-15	2.1	CVE-2009-3554 CONFIRM CONFIRM

[Back to top](#)

Last updated December 21, 2009


[Print This Document](#)